



February 4, 2019

TO: David S. Ferriero
Archivist of the United States

FROM: James Springs *James Springs*
Inspector General

SUBJECT: *Audit of National Archives and Records Administration's Fiscal Year 2018 Consolidated Financial Statements*
Audit Report No. 19-AUD-01

The Office of Inspector General (OIG) contracted with the independent certified public accounting firm CliftonLarsonAllen LLP (CLA) to audit the National Archives and Records Administration's (NARA) financial statements as of September 30, 2018 and 2017, and for the years then ended. On November 15, 2018, the OIG transmitted CLA's *Independent Auditors' Report* and the results of the OIG's oversight of the audit and review of that report. Additionally, on November 19, 2018 the OIG transmitted CLA's *FY 2018 Management Letter*.

This memorandum retransmits CLA's *Independent Auditors' Report, FY 2018 Management Letter*, and the results of the OIG's oversight of the audit. In addition, it transmits NARA's *Action Plan* and the *Office of Inspector General's Assessment of Management's Proposed Actions* (see page 12) to the recommendations in the audit report and management letter.

Results of the Independent Audit

Our contract with CLA required the audit be performed in accordance with generally accepted government auditing standards (GAGAS) and Office of Management and Budget Bulletin 19-01, *Audit Requirements for Federal Financial Statements*.

CLA issued an unmodified opinion on NARA's FY 2018 and 2017 financial statements. CLA found:

- The fiscal years 2018 and 2017 financial statements are presented fairly, in all material respects, in accordance with accounting principles generally accepted in the United States of America;
- No material weaknesses in internal control over financial reporting;
- One significant deficiency in internal control over financial reporting related to information technology controls; and
- No instances of noncompliance with certain provisions of laws, regulations, contracts and grant agreements.

Evaluation and Monitoring of Audit Performance

CLA is responsible for the attached auditor's report dated November 8, 2018, and the conclusions expressed in the accompanying report. To ensure the quality of the audit work performed, we evaluated the independence, objectivity, and qualifications of the auditors; reviewed the plan and approach of the audit; monitored the performance of the audit; reviewed CLA's report and related audit documentation; and inquired of its representatives. Our review, as differentiated from an audit in accordance with GAGAS, was not intended to enable us to express, as we do not express, an opinion on the financial statements or conclusions about the effectiveness of internal control over financial reporting or compliance with laws and regulations. Our review disclosed no instances where CLA did not comply, in all material respects, with GAGAS.

The report contains one recommendation aimed at improving NARA's information technology controls. In addition, the *FY 2018 Management Letter* contained two recommendations. Your office concurred with all of the recommendations. Based on your December 19, 2018 *Action Plan*, we considered all of the recommendations resolved and open. Once your office has fully implemented the recommendations, please submit evidence of completion of agreed upon corrective actions so that recommendations may then be closed.

As with all OIG products, we determine what information is publically posted on our website from the attached report. Consistent with our responsibility under the *Inspector General Act, as amended*, we may provide copies of our report to congressional committees with oversight responsibility over NARA.

We appreciate the cooperation and assistance NARA extended to us during the audit. Please call me or Jewel Butler, Assistant Inspector General for Audits, with any questions.

Attachments

cc: Debra Wall, Deputy Archivist of the United States
Micah Cheatham, Chief of Management and Administration
Colleen Murphy, Chief Financial Officer
Swarnali Haldar, Chief Information Officer
Kimm Richards, Accountability
United States House Committee on Oversight and Government Reform
Senate Homeland Security and Governmental Affairs Committee



CliftonLarsonAllen

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203
571-227-9500 | fax 571-227-9552
CLAconnect.com

INDEPENDENT AUDITORS' REPORT

Inspector General
National Archives and Records Administration

Archivist of the United States
National Archives and Records Administration

Report on the Financial Statements

We have audited the accompanying consolidated financial statements of the National Archives and Records Administration (NARA), which comprise the consolidated balance sheets as of September 30, 2018 and 2017, and the related consolidated statements of net cost and changes in net position, the combined statements of budgetary resources for the years then ended, and the related notes to the consolidated financial statements (financial statements).

Management's Responsibility for the Financial Statements

NARA management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America (U.S.); this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on these financial statements based on our audit. We conducted our audit in accordance with auditing standards generally accepted in the U.S.; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 19-01, *Audit Requirements for Federal Financial Statements* (OMB Bulletin 19-01). Those standards and OMB Bulletin 19-01 require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion on the Financial Statements

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the National Archives and Records Administration as of September 30, 2018 and 2017, and its net costs, changes in net position, and budgetary resources for the years then ended, in accordance with accounting principles generally accepted in the U.S.

Other Matters

Required Supplementary Information

Accounting principles generally accepted in the U.S. require that the information in the NARA's Management Discussion and Analysis (MD&A) and other Required Supplementary Information (RSI) sections be presented to supplement the financial statements. Such information, although not a part of the financial statements, is required by the Federal Accounting Standards Advisory Board (FASAB), which considers it to be an essential part of financial reporting for placing the financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the U.S., which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the financial statements, and other knowledge we obtained during our audits of the financial statements. We do not express an opinion or provide any assurance on this information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Information

Our audits were conducted for the purpose of forming an opinion on the financial statements as a whole. All other information exclusive of the financial statements, MD&A, and RSI such as the Letter from the Archivist of the United States, and the Other Information (OI) in Section 3 of the Agency Financial Report are presented for purposes of additional analysis and are not a required part of the financial statements. This information has not been subjected to the auditing procedures applied in the audits of the financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*

Internal Control over Financial Reporting

In planning and performing our audits of the financial statements, we considered NARA's internal control over financial reporting (internal control) to determine the audit procedures that were appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of NARA's internal control or on management's assertion on internal control included in the MD&A. Accordingly, we do not express an opinion on the effectiveness of NARA's internal control or on management's statement of assurance on internal control included in the MD&A.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of NARA's financial statements will not be prevented, or detected and corrected on a timely basis. A *significant deficiency* is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that have not been identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, we identified a deficiency in internal control, described below and in Exhibit A that we consider to be a significant deficiency.

Longstanding Control Deficiency in Information Technology Controls

NARA did not substantially address information technology control deficiencies that have existed since FY 2008. NARA not addressing these longstanding unresolved deficiencies impacts the effectiveness of NARA's information security program and internal controls over financial reporting. NARA did make some progress to mitigate these deficiencies, but more effort is needed.

Compliance with Laws, Regulations, Contracts, and Grant Agreements

As part of obtaining reasonable assurance about whether NARA's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements noncompliance with which could have a direct effect on the determination of material financial statement amounts and disclosures. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion.

The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported in accordance with *Government Auditing Standards* or OMB Bulletin 19-01.

Management's Responsibility for Internal Control and Compliance

NARA management is responsible for (1) evaluating the effectiveness of internal control over financial reporting based on criteria established under the Federal Managers' Financial Integrity Act (FMFIA), (2) providing a statement of assurance on the overall effectiveness on internal control over financial reporting, and (3) complying with other applicable laws, regulations, contracts, and grant agreements.

Auditors' Responsibilities

We are responsible for (1) obtaining a sufficient understanding of internal control over financial reporting to plan the audit, and (2) testing compliance with certain provisions of laws, regulations, contracts, and grant agreements.

We did not evaluate all internal controls relevant to operating objectives as broadly established by the FMFIA, such as those controls relevant to preparing statistical reports and ensuring efficient operations. We limited our internal control testing to testing controls over financial reporting. Because of inherent limitations in internal control, misstatements due to error or fraud, losses, or noncompliance may nevertheless occur and not be detected. We also caution that projecting our audit results to future periods is subject to risk that controls may become inadequate because of changes in conditions or that the degree of compliance with controls may deteriorate. In addition, we caution that our internal control testing may not be sufficient for other purposes.

We did not test compliance with all laws, regulations, contracts, and grant agreements applicable to NARA. We limited our tests to certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct effect on the determination of material financial statement amounts and disclosures. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. We caution that noncompliance may occur and not be detected by these tests and that such testing may not be sufficient for other purposes.

Management's Response to Audit Findings

Management's response to the findings identified in our report is presented in Exhibit B. We did not audit NARA's response and, accordingly, we express no opinion on it.

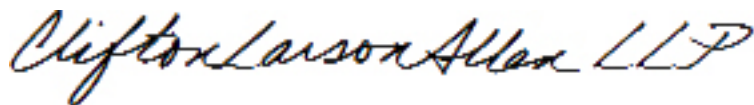
Status of Prior Year's Control Deficiencies and Noncompliance Issues

We have reviewed the status of NARA's corrective actions with respect to the findings included in the prior year's Independent Auditors' Report, dated November 8, 2017. The status of prior year findings is presented in Exhibit C.

Purpose of the Report on Internal Control over Financial Reporting and on Compliance

The purpose of the Report on Internal Control over Financial Reporting and on Compliance is solely to describe the scope of our testing of internal control and compliance and the result of that testing, and not to provide an opinion on the effectiveness of NARA's internal control or on compliance. These reports are an integral part of an audit performed in accordance with *Government Auditing Standards* in considering NARA's internal control and compliance. Accordingly, this report is not suitable for any other purpose.

CLIFTONLARSONALLEN LLP



Arlington, Virginia
November 8, 2018

EXHIBIT A
Significant Deficiency

**Longstanding Control Deficiency in Information Technology Controls
(Modified Repeat Finding)**

NARA relies extensively on information technology (IT) systems to accomplish its mission and in the preparation of its financial statements. Internal controls over these operations are essential to ensure the confidentiality, integrity and availability of critical data while reducing the risk of errors, fraud and other illegal acts. NARA's staff use IT systems to initiate and authorize financial transactions at the workstations, which transmit those transactions across the network to servers that record, process, summarize, and report financial transactions that support the preparation of its financial statements.

In FY 2018, NARA did not substantially address deficiencies in its IT general control categories of security management, access controls and configuration management that have existed since FY 2008. These longstanding unresolved deficiencies impact the effectiveness of NARA's information technology security program and internal controls over financial reporting.

A summary of key findings related to NARA Network (NARANet), Order Fulfillment and Accounting System (OFAS), and Records Center Program Billing System (RCPBS) systems are categorized and listed by general control category as follows:

Access Controls – We found prior year weaknesses related to account management unresolved. Instances of users with inactive accounts were identified along with instances of separated users who retained account access after their separation. In addition, weaknesses were found in regards to audit logging and incident response. It was noted that audit logs were not being retained for an entire year and not all security incidents were reported to US-CERT in a timely manner. Access controls should be established to ensure user accounts are effectively managed. In addition, incidents should be reported timely to mitigate the risk of subjecting systems to further exploits. Further, limited storage capacity can prevent NARA from conducting effective after-the-fact investigations of security incidents.

Security Management – We found prior year unresolved weaknesses related to system security plans which (a) were incomplete or not current; (b) plans of actions and milestones (POA&Ms) not updated timely; (c) missed milestone dates; or (d) contained incomplete data. Additionally, during FY 2018, we found that (a) system assessment reports did not have the recommended countermeasures for all failed controls; and (b) policies and procedures were not properly reviewed and approved. Security management controls provide the framework for the continual assessment of risk, development of security procedures and monitoring the implementation effectiveness of those procedures.

Configuration Management – We found that while there were improvements in this area compared to FY2017, configuration management weaknesses associated with vulnerability and patch management continue to exist. Specifically, we found prior year unresolved weaknesses related to the detection, remediation, and monitoring of known vulnerabilities for software patches and updates. Additionally, system configuration weaknesses existed on servers and workstations. Further, change management procedures for testing and approving system changes were not consistently implemented. Absent an effectively implemented and enforced configuration management program that addresses significant security weaknesses, there is an increased risk that financial information may be inadvertently or deliberately disclosed, manipulated, or misappropriated.

We believe that the IT control deficiencies resulted from inadequate resources, as well as

EXHIBIT A Significant Deficiency

inadequate communication and oversight by NARA management. Management has been in the process of deploying an Information System Security Officer (ISSO) contract since FY 2017 to remediate these weaknesses, however, these efforts were still ongoing during FY 2018.

Our testing was based on the following key criteria:

- National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, “*Security and Privacy Controls for Federal Information Systems and Organizations*”
 - SI-2 Flaw Remediation
The organization identifies information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.
 - SA-22 Unsupported System Components
The organization replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer;
 - CA-5 Plans of Action and Milestones
The organization develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
- The NARA Cybersecurity Framework Methodology, under Task 4.2: Update Risk Assessment, states:
 - “Risk assessment are updated annually or whenever there are significant changes to the information system or environment of operations (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.”
- OMB Memorandum A-130, Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources*
 - Establishes minimum requirements for Federal Information Programs and assigned Federal agency responsibilities for the security of information and information systems. The Circular specifically prohibits agencies from the use of unsupported information systems and system components, and requires agencies to ensure that systems and components that cannot be appropriately protected or secured are given high priority for upgrade or replacement. In addition, the Circular requires agencies to implement and maintain current updates and patches for all software and firmware components of information systems. Additionally, the Circular requires system security plans to be consistent with guidance issued by NIST.

These weaknesses could be potentially exploited, intentionally or unintentionally, to undermine the integrity and completeness of data processed by NARA’s financial management systems, including its feeder systems.

EXHIBIT A
Significant Deficiency

Recommendations:

- 1) We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to:
 - a. Ensure user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements (repeat recommendation).
 - b. Increase NARANet storage capacity to enable retention of NARANet events in accordance with NARA policy.
 - c. Ensure that all incidents are reported to US-CERT within one hour of discovery.
 - d. Ensure Security Assessment Reports are updated with summaries of test failures for all failed controls identified.
 - e. Ensure security documentation such as system security plans are reviewed and updated on an annual basis, for each system (repeat recommendation).
 - f. Ensure plans of actions and milestones are created, updated and remediated, for each system, in accordance with NARA policies, guidance and directives (repeat recommendation).
 - g. Implement remediation efforts to address security deficiencies identified during our assessments of NARA's database platforms and network infrastructure (repeat recommendation).
 - h. Fully complete the migration of applications to vendor supported operating systems (repeat recommendation).
 - i. Ensure all changes are tested and properly approved before being moved into the production environment.

EXHIBIT B
Management's Response



ARCHIVIST *of the*
UNITED STATES

DAVID S. FERRIERO
T: 202.357.5900
F: 202.357.5901
david.ferriero@nara.gov

Date: November 8, 2018

To: James Springs
Inspector General

From: David S. Ferriero
Archivist of the United States

Subject: Management Response to the FY2018 Financial Statement Audit

Thank you for the opportunity to review your *Independent Auditor's Report* on the financial statement audit of the National Archives and Records Administration for the fiscal year ending September 30, 2018.

I am pleased to have received an unmodified or "clean" independent audit opinion on our financial statements. An unmodified opinion recognizes NARA's commitment to producing accurate and reliable financial statements and supports our efforts to continuously improve our financial management program.

NARA acknowledges the Information Security challenges identified in this report and concurs with the recommendation of the independent auditor. NARA self-identified IT security as a material weakness in internal controls and a summary of our corrective action plan is included in the FY 2018 Statement of Assurance. I appreciate the work performed by the auditor in this area and will ensure the auditor's findings and recommendation are incorporated into NARA's action plan.

I would like to thank the Office of Inspector General and CliftonLarsonAllen LLP for their cooperative and professional approach in the conduct of this audit.

DAVID S. FERRIERO
Archivist of the United States

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20408-0001
www.archives.gov

EXHIBIT C
Status of Prior Year Recommendations

Our assessment of the current status of the recommendations related to findings identified in the prior year audit is presented below:

<i>FY 2017 Recommendation</i>	<i>Type</i>	<i>Fiscal Year 2018 Status</i>
a. Strengthen controls for internal website password transmission and encryption to include Hyper Text Transfer Protocol Secure (HTTPS) and Secure Socket Layer (SSL) technologies.	Significant Deficiency 2017	Closed.
b. Strengthen the review and disabling of user accounts in accordance with NARA's information technology policies and requirements.	Significant Deficiency 2017	In process; see 2018 Significant Deficiency, recommendation "a"
c. Implement enhanced processes to secure physical access controls to sensitive areas.	Significant Deficiency 2017	Closed
d. Continue to implement improved processes for reviewing and updating key security documentation, including system security plans on an annual basis.	Significant Deficiency 2017	In process; see 2018 Significant Deficiency, recommendation "e"
e. Implement improved processes for creating, updating and remediating plans of actions and milestones.	Significant Deficiency 2017	In process; see 2018 Significant Deficiency, recommendation "f"
f. Implement remediation efforts to address security deficiencies identified during our assessments of NARA's database platforms and network infrastructure.	Significant Deficiency 2017	In process; see 2018 Significant Deficiency, recommendation "g"
g. Fully complete the migration of applications to vendor supported operating systems.	Significant Deficiency 2017	In process; see 2018 Significant Deficiency, recommendation "h"



FISCAL YEAR 2018 MANAGEMENT LETTER

To the Inspector General
National Archives and Records Administration

To the Archivist
National Archives and Records Administration

In planning and performing our audit of the consolidated financial statements of the National Archives and Records Administration (NARA) as of and for the year ended September 30, 2018, in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial statement audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No.19-01, *Audit Requirements for Federal Financial Statements* (OMB Bulletin 19-01), we considered NARA's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of NARA's internal control. Accordingly, we do not express an opinion on the effectiveness of NARA's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified. In addition, because of inherent limitations in internal control, including the possibility of management override of controls, misstatements due to fraud or error may occur and not be detected by such controls.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our Independent Auditors' Report, dated November 8, 2018, described a significant deficiency identified during our audit. However, during our audit we also became aware of deficiencies in internal control other than significant deficiencies and material

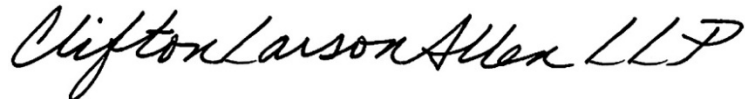
Communication with Management

weaknesses and other matters that represent opportunities for strengthening internal control and operating efficiency. While the nature and magnitude of these other deficiencies in internal control were not considered important enough to merit the attention of those charged with governance, they are considered of sufficient importance to merit management's attention. Our comments and recommendations regarding those matters are summarized in Appendix A (Management Letter). This communication does not affect our Independent Auditors' Report, dated November 8, 2018, which contains our written communication of a significant deficiency that came to our attention in performing our audit.

We have already discussed these comments and recommendations with various NARA personnel, and we will be pleased to discuss them in further detail at your convenience.

Appendix B presents the current year status of the prior year management letter comments. This communication is intended solely for the information and the use of NARA management and NARA Office of Inspector General and is not intended to be, and should not be, used by anyone other than these specified parties.

CliftonLarsonAllen LLP

A handwritten signature in cursive script that reads "CliftonLarsonAllen LLP".

Arlington, Virginia
November 8, 2018

Appendix A
National Archives and Records Administration
Fiscal Year 2018 Financial Statement Audit

Management Letter Comments

1. Entity Wide Travel Policy was not Updated Timely [NFR 2016-03/2018-01] (Repeat Finding)

During fiscal year (FY) 2016 audit, we noted that NARA's 601 Travel Policy and Procedures listed on NARA's intranet and provided to the auditors was not current. The policy refers to and provides instructions for the use of GovTrip. NARA migrated to Concur CGE in June of 2014.

This policy still had not been updated as of September 30, 2018. Errors could occur in the processing of travel transactions if employees refer to outdated policies and procedures in the performance of their duties.

According to management, the review and update process of the policies and procedures is an on-going process. Also, many of the policies and procedures were written specifically for a process related to systems and were not updated for technology changes due to time availability.

Recommendation 1:

We recommend that management update the travel policy to ensure that all written policies and procedures are reviewed and revised timely.

Management Response:

Management concurred with the findings and recommendation without additional comment.

2. Lack of Reconciliation between Maximo and Subsidiary Ledger [NFR 2016-04/2018-02] (Modified Repeat Finding)

In our FY2016 audit, we reviewed the validation of Property Accountable Officer (PAO) physical accountable property and equipment inventory to Maximo's record completion log for the period of October 1, 2015 through June 30, 2016. During the review, we noted the amount from Maximo is \$85.8 million less than the subsidiary ledger balance for equipment account 1750 from Oracle.

We recommended management implement a reconciliation process to identify and document the differences between the total cost of assets record in Maximo and the Property and Equipment (P&E) sub-ledger in Oracle.

In FY2017, in response to our finding, management implemented a process to reconcile the P&E subsidiary ledger to Maximo using the bar code and the Business Owner's confirmation. We reviewed the reconciliation and noted approximately

Appendix A
National Archives and Records Administration
Fiscal Year 2018 Financial Statement Audit

Management Letter Comments

\$17.2 million of the total \$54.5 million cost of assets recorded in the P&E subsidiary ledger have “#N/A” in the data cells for the corresponding Maximo data. According to management, these assets could not be validated in Maximo based on the bar code number. These items will require further research and work with the Business Owner to reconcile.

In fiscal year 2018, we reviewed the FY18 PP&E subsidiary ledger to Maximo reconciliation as part of follow up on prior year finding. We noted approximately \$7.9M of \$63.2M total cost of assets recorded in the PP&E subsidiary ledger have “#N/A” in the data cells for the corresponding Maximo data. According to management, these assets could not be validated in Maximo based on the bar code number.

Inadequate reconciliation to ensure that the records kept in Maximo reflect those in subsidiary ledger could cause NARA to be relying on incomplete or inaccurate data which could impact its P&E balance reported on the financial statements. Since NARA performs their inventory of accountable assets from the Maximo system, without a reconciliation of the two systems, there is the potential that items disposed of and removed from Maximo were not recorded in the subsidiary ledger.

Recommendation 2:

We recommend that management complete the reconciliation process to identify and document the differences between the assets record in Maximo and the PP&E sub-ledger in Oracle to ensure reliability and completeness of the sub-ledger detail.

Management Response:

Management concurred with the finding and recommendation without additional comment.

Appendix B
National Archives and Records Administration
FY2018 Financial Statement Audit
Status of Prior Year Findings

Prior Finding	Fiscal Years 2016 and 2017 Findings	Prior Finding Description	Fiscal Year 2018 Status
2016-03	Entity Wide Travel Policy is not updated timely	NARA's 601 Travel Policy and Procedures listed on NARA's intranet and provided to the auditors is not current.	Open. Repeat finding in FY 2018
2016-04	Lack of Reconciliation between Maximo and Subsidiary Ledger	There is no reconciliation performed between Maximo to the subsidiary ledger to ensure that the completeness and accuracy of the accountable property in Maximo is properly reflected in the subsidiary ledger.	Open. Modified repeat finding in FY 2018
2017-01	Aged obligation should have been de-obligated	Untimely de-obligation of inactive obligation.	Closed

Office of Inspector General's Assessment of Management's Proposed Actions

On November 15, 2018, the OIG transmitted CLA's report of the results of the audit of NARA's financial statements as of September 30, 2018 and 2017, and for the years then ended. On December 19, 2018, the OIG received NARA's *Action Plan* to Recommendation 1 in the report and two other recommendations documented in CLA's *FY 2018 Management Letter*. We assessed management's proposed actions and consider them responsive to CLA's recommendations. The recommendations will remain open and resolved pending completion of the corrective actions.

Finding 1, Recommendation 1a-1i

We recommend that the NARA Chief Information Officer continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to:

Recommendation 1a: Ensure user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements (repeat recommendation).

Management Response

Information Services will assign an Information System Security Officer (ISSO) for each information system and ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 1b: Increase NARANet storage capacity to enable retention of NARANet events in accordance with NARA policy.

Management Response

Information Services will increase the storage capacity available for its Tenable Log Correlation Engine (LCE) audit log storage and correlation solution to ensure sufficient capacity exists to maintain logs for at least 1 year. Information Services will either acquire storage space through the agency's storage area network (SAN) or through adding additional physical storage capacity directly to the LCE server.

Target Completion Date: March 29, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 1c: Ensure that all incidents are reported to US-CERT within one hour of discovery.

Management Response

Information Services will ensure incidents are reported to United States Computer Emergency Readiness Team (US-CERT) within one hour of being identified by the Computer Incident Response Team (CIRT).

Target Completion Date: October 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 1d: Ensure Security Assessment Reports are updated with summaries of test failures for all failed controls identified.

Management Response

Information Services will update Security Assessment Reports to document a summary of failed test controls identified in Security Assessment Reports.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 1e: Ensure security documentation such as system security plans are reviewed and updated on an annual basis, for each system (repeat recommendation).

Management Response

This action is dependent on obtaining additional funding for ISSO's one year prior to being able to close out the recommendation. Information Services will assign an ISSO for each NARA information system. The ISSOs will ensure System Security Plans (SSP) are reviewed and updated for all NARA systems in accordance with NARA policy.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 1f: Ensure plans of actions and milestones are created, updated and remediated, for each system, in accordance with NARA policies, guidance and directives (repeat recommendation).

Management Response

Information Services will assign an ISSO for each NARA information system. The ISSOs will ensure all systems have POA&Ms created when weaknesses are identified, to include completion dates; are remediated in a timely manner; and are updated to include detailed information on the status of the corrective actions.

Target Completion Date: October 30, 2020

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 1g: Implement remediation efforts to address security deficiencies identified during our assessments of NARA's database platforms and network infrastructure (repeat recommendation).

Management Response

Information Services will continue its efforts to accomplish security and control objectives. Information Services will work with system owners and ISSOs to coordinate remediation efforts to address security deficiencies.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 1h: Fully complete the migration of applications to vendor supported operating systems (repeat recommendation).

Management Response

Information Services will ensure all information systems migrate away from [REDACTED] to vendor supported operating systems.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 1i: Ensure all changes are tested and properly approved before being moved into the production environment.

Management Response

NARA will ensure applicable Requests for Change (RFCs) are tested, with evidence of test results, before Enterprise Change Advisory Board (ECAB) approval. There are cases when the only real test of the change is when the change is made in the production environment (e.g. a DNS change). In that case, test plans will not be available prior to going to ECAB and this will be documented in the RFC.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 2: We recommend that management update the travel policy to ensure that all written policies and procedures are reviewed and revised timely.

Management Response

Accounting Policy and Operations will update NARA's travel policy.

Target Completion Date: September 30, 2019

OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.

Recommendation 3: We recommend that management complete the reconciliation process to identify and document the differences between the assets record in Maximo and the PP&E sub-ledger in Oracle to ensure reliability and completeness of the sub-ledger detail.

Management Response

Financial Reporting will substantially complete the PP&E subledger to MAXIMO reconciliation by September 30, 2019. XF plans to institute processes for ongoing monitoring and reconciliation to address any new disposals going forward.

Target Completion Date: September 30, 2019

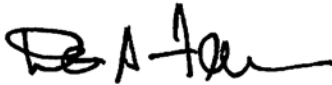
OIG Analysis

We consider NARA's proposed action responsive to CLA's recommendation. This recommendation will remain open and resolved pending completion of the corrective actions identified above.



Date: DEC 19 2018
To: James Springs, Inspector General
From: David S. Ferriero, Archivist of the United States
Subject: Action Plan to OIG Report 19-AUD-01, *Audit of NARA's Fiscal Year 2018 Consolidated Financial Statements*

Attached is our action plan for the three recommendations included in the subject audit report and Management Letter. As each recommendation is completed, we will provide documentation to your office. If you have questions about this action plan, please contact Kimm Richards at kimm.richards@nara.gov or by phone at 301-837-1668.



DAVID S. FERRIERO
Archivist of the United States

Attachment

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION
8601 ADELPHI ROAD
COLLEGE PARK, MD 20740-6001
www.archives.gov

**Action Plan Response to OIG Report 19-AUD-01,
Fiscal Year 2018 Consolidated Financial Statements**

Recommendation 1a (I): We recommend the NARA CIO continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to ensuring user accounts are reviewed and disabled in accordance with NARA's information technology policies and requirements (repeat recommendation).

Planned Action: Information Services will assign an Information System Security Officer (ISSO) for each information system and ensure user system accounts for all systems are periodically reviewed and automatically disabled in accordance with NARA policy.

Target Completion Date: October 30, 2020

Recommendation 1b (I): We recommend the NARA CIO continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to increasing NARANet storage capacity to enable retention of NARANet events in accordance with NARA policy.

Planned Action: Information Services will increase the storage capacity available for its Tenable Log Correlation Engine (LCE) audit log storage and correlation solution to ensure sufficient capacity exists to maintain logs for at least 1 year. Information Services will either acquire storage space through the agency's storage area network (SAN) or through adding additional physical storage capacity directly to the LCE server.

Target Completion Date: March 29, 2019

Recommendation 1c (I): We recommend the NARA CIO continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to ensuring that all incidents are reported to US-CERT within one hour of discovery.

Planned Action: Information Services will ensure incidents are reported to United States Computer Emergency Readiness Team (US-CERT) within one hour of being identified by the Computer Incident Response Team (CIRT).

Target Completion Date: October 30, 2019

Recommendation 1d (I): We recommend the NARA CIO continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to ensuring Security Assessment Reports are updated with summaries of test failures for all failed controls identified.

Planned Action: Information Services will update Security Assessment Reports to document a summary of failed test controls identified in Security Assessment Reports.

Target Completion Date: September 30, 2019

Recommendation 1e (I): We recommend the NARA CIO continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to ensuring security documentation such as system security plans are reviewed and updated on an annual basis, for each system (repeat recommendation).

Planned Action: This action is dependent on obtaining additional funding for ISSO's one year prior to being able to close out the recommendation. Information Services will assign an ISSO for each NARA information system. The ISSOs will ensure System Security Plans (SSP) are reviewed and updated for all NARA systems in accordance with NARA policy.

Target Completion Date: October 30, 2020

Recommendation 1f (I): We recommend the NARA CIO continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to ensuring plans of actions and milestones are created, updated and remediated, for each system, in accordance with NARA policies, guidance and directives (repeat recommendation).

Planned Action: Information Services will assign an ISSO for each NARA information system. The ISSOs will ensure all systems have POA&Ms created when weaknesses are identified, to include completion dates; are remediated in a timely manner; and are updated to include detailed information on the status of the corrective actions.

Target Completion Date: October 30, 2020

Recommendation 1g (I): We recommend the NARA CIO continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to implementing remediation efforts to address security deficiencies identified during our assessments of NARA's database platforms and network infrastructure (repeat recommendation).

Planned Action: Information Services will continue its efforts to accomplish security and control objectives. Information Services will work with system owners and ISSOs to coordinate remediation efforts to address security deficiencies.

Target Completion Date: September 30, 2019

Recommendation 1h (I): We recommend the NARA CIO continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to fully completing the migration of applications to vendor-supported operating systems (repeat recommendation).

Planned Action: Information Services will ensure all information systems migrate away from [REDACTED] to vendor-supported operating systems.

Target Completion Date: September 30, 2019

Recommendation 1i (I): We recommend the NARA CIO continue to analyze and prioritize remediation efforts to accomplish security and control objectives. Key tasks should include, but are not limited to ensuring all changes are tested and properly approved before being moved into the production environment.

Planned Action: NARA will ensure applicable Requests for Change (RFCs) are tested, with evidence of test results, before Enterprise Change Advisory Board (ECAB) approval. There are cases when the only real test of the change is when the change is made in the production environment (e.g. a DNS change). In that case, test plans will not be available *prior* to going to ECAB and this will be documented in the RFC.

Target Completion Date: September 30, 2019

Recommendation 2 (X): We recommend that management update the travel policy to ensure that all written policies and procedures are reviewed and revised timely.

Planned Action: Accounting Policy and Operations will update NARA's travel policy.

Recommendation 3 (X): We recommend that management complete the reconciliation process to identify and document the differences between the assets record in Maximo and the PP&E sub-ledger in Oracle to ensure reliability and completeness of the sub-ledger detail.

Planned Action: Financial Reporting will substantially complete the PP&E subledger to MAXIMO reconciliation by September 30, 2019. XF plans to institute processes for ongoing monitoring and reconciliation to address any new disposals going forward.

Target Completion Date: September 30, 2019